A FEDERAL CYBER CENTER

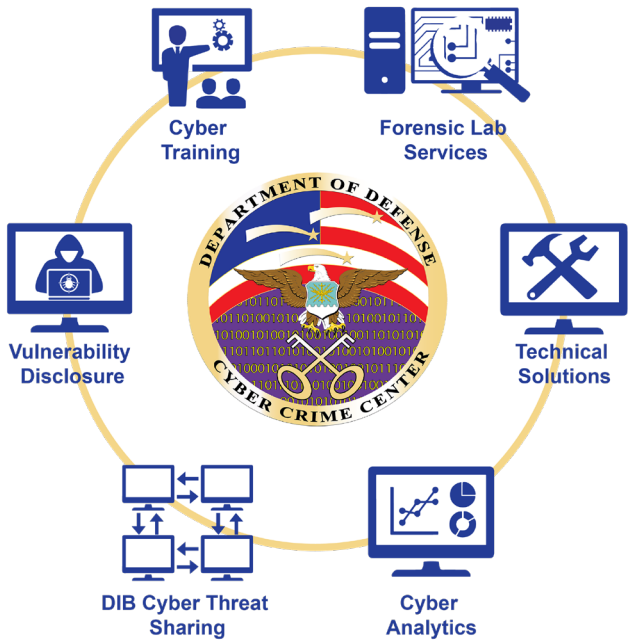
DoD CYBER CRIME CENTER (DC3)

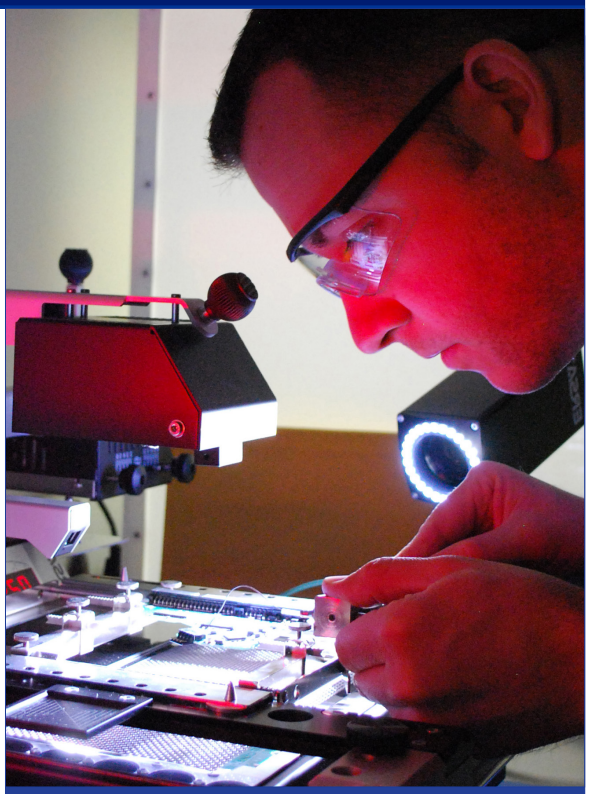
FACT SHEET

DoD CYBER CRIME CENTER (DC3)

Established as an entity within the Department of the Air Force in 1998, DC3 provides digital and multimedia (D/MM) forensics, specialized cyber training, technical solutions development, and cyber analytics for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection (CIP); law enforcement and counterintelligence (LE/CI); document and media exploitation (DOMEX), counterterrorism (CT) and safety inquiries. DC3 delivers superior results by synthesizing its six functional directorate's expertise into a unique holistic capability.

DC3 is designated as a federal cyber center by National Security Presidential Directive 54/Homeland Security Presidential Directive 23, as a DoD center of excellence for D/MM forensics by DoD Directive 5505.13E, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIB CS Program; 32 CFR Part 236). DC3 delivers capability with a team comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized support.





A DC3 lab specialist extracts data from damaged media: one of the most challenging but important services the lab provides.

DC3 hosts embedded liaisons from numerous mission partners, to include DoD LE/CI organizations, the National Security Agency, U.S. Cyber Command, four distinct Damage Assessment Management Offices (Office of the Secretary of Defense and the three Military Departments), a Joint Acquisition Protection & Exploitation Cell, and an Air Force Life Cycle Management Center element. DC3 also maintains enduring partnerships with the Federal Bureau of Investigation, the National Media Exploitation Center, and other core mission partners via embedded DC3 liaisons.

DoD CYBER CRIME CENTER
410-981-6610 | www.dc3.mil | info@dc3.mil
@DC3Forensics
@DC3 Cyber Crime Center

OPERATIONS

Cyber Forensics Laboratory (CFL) — CFL performs D/MM forensic examinations, device repair, data extraction and expert testimony for the DoD. The lab's robust intrusion and malware analysis capability also supports other DC3 lines of business and specifically to DoD LE/CI organizations. CFL expanded its capabilities by adding unlock services for mobile devices, and has experienced a 97 percent unlock success rate since launching this service. CFL is the largest DoD D/MM lab and is accredited under ISO 17025 by the ANSI National Accreditation Board (ANAB), which guides reliable, repeatable and valid exam procedures, subjected to quality control and peer review.

Cyber Training Academy (CTA) — The training academy provides classroom and web-based cyber training through more than 30 unique courses to DoD entities that protect DoD information systems from unauthorized, criminal, fraudulent and foreign intelligence intrusions. The academy confers DoD certifications in digital forensics and cyber investigations. To complement its in-residence training, the academy has an extensive distance learning program (DCITA.edu) and has formal relationships with 16 institutions of higher learning. During FY20, the academy delivered a total of 448,504 hours of training from in-residence and online learning offerings to students with duties in DoD LE/CI, Cybersecurity, Intelligence, and Cyber Mission Forces.

Analytical Group (AG) — AG conducts sharply focused technical, all-source, and foreign language-enabled cyber threat analysis in support of law enforcement/counterintelligence (LE/CI) investigations and operations, and U.S. Intelligence Community requirements. The AG also leads collaborative analytical and technical exchanges with subject matter experts from numerous DoD, Federal LE/CI, Computer Network Defense, USIC and cybersecurity agencies to build a tailored operating picture of high-priority cyber threats.

Department of Defense-Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment (DCISE) — DCISE assists over 760 companies in a voluntary partnership to understand the risks from nation-state threats and aids them in elevating their cybersecurity to better safeguard unclassified DoD information residing on or transiting their corporate networks. As the DoD operational hub for this effort, DCISE provides partner companies actionable indicators for their network defense systems (nearly 446K so far) and tailored analyses to aid remediation efforts for cyber incidents. Supported by the CFL, partner companies have benefited from over 74,000 hours of no-cost intrusion forensics and malware reverse engineering products and services. To enhance partner cybersecurity expertise, DCISE also delivers face-to-face consults with company cybersecurity analysts and executives, and conducts interactive group technical exchanges with partner cybersecurity experts. DCISE is also the designated DoD repository for all defense contractor cyber incident reporting under DFARS 252.204-7012 requirements.

Technical Solutions Development (TSD) — As DC3's technical solutions development capability, TSD tailors software and system solutions to support digital forensic examiners and cyber intrusion analysts, including AG, DCISE, CFL and VDP, with tools and techniques engineered to their specific requirements. TSD also develops tools such as DC3 Advanced Carver to aid data extraction for various DoD requirements such as DOMEX. TSD conducts test and validation services on commercial off-the-shelf, government off-the-shelf, hardware and in-house developed software before use in a forensic process (a prerequisite for lab accreditation).

Vulnerability Disclosure Program (VDP) — The Secretary of Defense directed DC3 to begin VDP operation in 2016, to better align with private industry. Supporting the DoD Chief Information Officer, U.S. Cyber Command, Joint Force HQs–DoDIN, and the cyber elements of all DoD components, the VDP crowdsources the expertise of private-sector cyber security researchers to identify vulnerabilities on DoD information systems. VDP analyzes, triages, and corroborates vulnerabilities submitted to the program, coordinates with the system owners for mitigation, and then validates the technical effectiveness of their mitigation actions. VDP provides an independent assessment of DoDIN security and defensive measures, discovers vulnerabilities not found by existing red-team or automated systems, and identifies noncompliance with technical standards. Follow us on Twitter @DC3VDP.